REMARKS:

Independent claims 4, 12, 16, 21, 31, 53, 57, and 70 (each of which claims a system) and dependent claim 11 are hereby canceled and replaced respectively by new independent claims 88, 90, 91, 92, 93 (and 94), 97, 98, 99 (and 100), and 89. New dependent claims 95, 96, and 101-104 are also hereby added, and claims 1, 3, 10-11, 15, 18, 19, 23, 24, 35, 36, 55, 57, 73, 74, and 78 are also hereby canceled.

Claims 1-3, 9, 11, 14, 16, 27-29 (and apparently also 30), 31, 53, 57, and 75-76 have been objected to on the ground that the abbreviation "TMDS" is not defined and "must be defined, at least once in the first appearance" and claims 27-30 have been objected to on the ground that "AES" and "HDCP" are not defined. In response, claims 2, 6, 7, 14, 27-29, 75, and 87 are hereby amended (and the new claims are drafted) to define "TMDS," "AES," and "HDCP" as they are defined in the specification, where each such expression first appears in each relevant group of claims. Claim 1 is hereby canceled.

Claims 1-36, 53-57, and 70-87 stand rejected under 35 U.S.C. 112, second paragraph as being indefinite. In response, Applicant respectfully contends that the uncanceled ones of these claims as amended (and the new claims) satisfy the requirements of 35 U.S.C. 112 for the following reasons. Claims 1, 36, and 78 are hereby canceled.

In response to the assertion in the Office Action that the phrase "TMDS-like" link renders claims 1-3, 9, 11, 14, 16, 21, 27-29, 31, 40, 53, 57, 63, 75-76, and 87 indefinite because each such claim includes elements not actually recited but implied or encompassed by the phrase "TMDS-like" link, Applicant contends that the uncanceled ones of these claims as amended (and the new claims) satisfy the requirements of 35 U.S.C. 112 for the following reasons.

At page 8, the specification of the present application defines the phrase "TMDS-like link" as:

> a serial link, capable of transmitting digital video data (and a clock for the digital video data) from a transmitter to a receiver, and optionally also transmitting one or more additional signals ... between the transmitter and receiver, that is or includes either a TMDS link or a link having some but not all of the characteristics of a TMDS link.

According to this definition, a TMDS link is an example of a TMDS-like link. A TMDS link (e.g., the TMDS link of Fig. 1) is designed to be connected between a transmitter (e.g., transmitter 1 of Fig. 1) and a receiver (e.g., receiver 3 of Fig. 1), and includes four conductor pairs (as well as additional conductors): three conductor pairs that implement video channels ("Channel 0," "Channel 1," and "Channel 2" of Fig. 1); and a fourth conductor pair that implements a clock channel ("Channel C" of Fig. 1). Encoded video data and a video clock signal are transmitted as differential signals over the conductor pairs, with signal transmission over the conductor pairs typically occurring in one direction only from a transmitter to a receiver. Other examples of TMDS-like links that are not TMDS links are described in the application's specification. Although different TMDS-like links may have different numbers of conductors, may transmit digital video data in different formats (e.g., unencoded digital video, or digital video encoded in any of a variety of different ways), and may transmit data other than digital video data (as well as digital video data and a clock for digital video data), the definition of "TMDS-like link" is believed to be unambiguous.

Applicant does not intend that any of the rejected claims as amended (or any of the new claims) must include any element in addition to the elements explicitly recited therein. The recited expression "TMDS-like link" is defined unambiguously in the specification. Thus, Applicant contends that the claims are unambiguous and satisfy the requirements of 35 U.S.C. 112.

Neither the MPEP section cited in support of the rejection (MPEP Section 2173.05(d)) nor any statute or regulation prohibits use in claims of a phrase whose meaning is clear from supporting description in the specification. Because the expression "TMDS-like link" is defined unambiguously in the specification, it is used properly in the claims. Applicant respectfully requests that the Examiner identify any element that the Examiner contends is necessarily included but not recited in any of claims 2, 9, 14, 27-29, 40, 63, 75-76, and 87, as amended (and the new claims), unless the rejection under 35 U.S.C. 112, second paragraph, is withdrawn.

In response to the rejection of claim 57, Applicant notes that corresponding new claim 98 recites an external agent configured to be coupled to a transmitter and a receiver, where the transmitter is configured to operate in a pass-through mode, and the receiver is configured to operate in a non-decrypting mode. Claim 98 recites that in the non-decrypting mode, the

receiver does not decrypt any data that it receives over a link. The claim does not require that the transmitter be in any specific mode when the receiver is in the non-decrypting mode. In the pass-through mode, the transmitter receives data from a source and transmits the data to the receiver without encrypting said data. The claim does not recite that the transmitter is "operable" in such pass-through mode. The claim is believed to be unambiguous and does not recite that the operation of receiving data from the recited source is the recited pass-through mode (as speculated in the office action).

In response to the rejection of claim 9, Applicant notes that claim 9 as amended recites a switch coupled to assert encrypted data (received from a transmitter) over a selected one of a third TMDS-like link and a fourth TMDS-like link. Applicant intends that this limitation be given its plain meaning (which is consistent with the definition of "switch" provided in the specification, in the sentence that spans page 15 and 16 of the specification), which assumes that the switch has at least two states: a state in which one TMDS-like link has been selected and the switch forwards the encrypted data that it has received to that TMDS-like link; and another state in which another TMDS-like link has been selected and the switch forwards the encrypted data that it has received to that other TMDS-like link.

In response to the rejection of claims 74 and 82, Applicant notes that the "key material" recited in claim 82 (and new claim 102) and described in the specification (for example, at page 10, lines 26-27) is data for use by at least one of a transmitter and a receiver in an encryption and/or decryption process.

In response to the rejection of claims 75 and 84, Applicant intends that the recitation therein (and in new claim 103) that a receiver decrypts (or can decrypt) encrypted data "in response to" a receiver key be given its plain meaning, denoting that the receiver decrypts (or can decrypt) the encrypted data using the receiver key.

Claim 30 is amended in response to the rejection thereof under 35 U.S.C. 112. Applicant notes that the abbreviation "AES" in the "AES-128 CTR protocol" recited in claim 30 is defined in amended claim 29, and that recited "AES-128 CTR protocol" denotes a counter ("CTR") mode of a version of an AES protocol that uses a 128-bit key to generate a sequence of 128-keys (a key schedule), and encrypts (or decrypts) each block of data in a

sequence of ten rounds using the keys of the key schedule, as described in the first full paragraph of page 38 of the specification and the first full paragraph of page 41 of the specification.

Claims 70-76 and 78-85 stand rejected under 35 U.S.C. 102(b) as being anticipated by pages 400-401 of the book by Menezes, et al., entitled Handbook of Applied Cryptography ("Menezes"). In response, claims 70, 73, 74, and 78 are canceled, and Applicant contends that new claims 99-104 and claims the uncanceled ones of claims 70-76 and 78-85 as amended are patentable over Menezes for the following reasons.

Menezes fails to teach or suggest any of the following limitations of claim 99 or 100:

A transmitter (or receiver) for use in a system including a communication channel and a receiver (or transmitter), wherein the transmitter and receiver are configured to implement a content protection protocol that includes a procedure for supplying a receiver key to the receiver, and a challenge-response procedure for verifying whether the transmitter has a transmitter key matching the receiver key,

a receiver configured to encrypt first data in accordance with a content protection protocol using a receiver key to generate an authentication message, and to send the authentication message to a transmitter over a communication channel between the transmitter and the receiver; and

a transmitter configured to perform a predetermined mathematical function on the authentication message to generate a result, to encrypt the result using a transmitter key to generate an encrypted result, and to send the encrypted result to the receiver over the channel; and

a receiver configured to generate a decrypted result by decrypting the encrypted result using the receiver key, and to determine whether the decrypted result satisfies a predetermined criterion.

Menezes also fails to teach or suggest operating a transmitter and a receiver to perform a challenge-response procedure to determine whether at least one of a transmitter key and a receiver key satisfies a predetermined criterion, thereby determining whether the receiver key has a predetermined relationship to the transmitter key, including by performing the following steps of amended claim 80:

(d) operating the receiver to encrypt first data in accordance with the protocol using the receiver key to generate an authentication message;

(e) sending the authentication message to the transmitter;

(f) operating the transmitter to perform a predetermined mathematical function on the authentication message to generate a result, and to encrypt the result using the transmitter key to generate an encrypted result;

(g) sending the encrypted result to the receiver; and

(h) operating the receiver to generate a decrypted result by decrypting the encrypted result using the receiver key.

Menezes discloses several challenge-response procedures. However, none of them includes above-noted limitations of claim 99, 100, or 80. For example, even if one assumes that entity "B" in Section 10.16 of Menezes is a receiver and that entity "A" in Section 10.16 is a transmitter, Menezes apparently includes no teaching or suggestion that such a receiver should encrypt any "first data" (e.g., Menezes includes no teaching or suggestion that a receiver should encrypt random number rB) to generate an authentication message, or that such a transmitter should perform a predetermined mathematical function on such an authentication message to generate a result and then encrypt the result and send the encrypted result to the receiver. If one assumes that entity "B" in Section 10.16 of Menezes is a transmitter and that entity "A" in Section 10.16 is a receiver, then Menezes includes no teaching or suggestion that the transmitter should perform a predetermined mathematical function on any authentication message received from entity "A" to generate a result, encrypt the result using a transmitter key to generate an encrypted result, or send the encrypted result to entity "A."

Nor does Menezes teach or suggest that a transmitter should send encrypted data over a TMDS-like link to a receiver and that the receiver should decrypt the encrypted data in response to a receiver key and a sequence of count values, wherein the transmitter is configured to generate a pseudo-random value, the transmitter is configured to transmit the pseudo-random value over one of a communication channel and a TMDS-like link to the receiver, and the receiver is configured to include the pseudo-random value as a field of at

least one of the count values upon determining that the decrypted result satisfies a predetermined criterion, as recited in claim 75.

Claims 77 and 86-87 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes in view of pages 101, 131-132, 140-141, 262, 386-387, 389, and 406 of the book by Pfleeger entitled Security in Computing ("Pfleeger"). In response, Applicant contends that these claims are patentable over the cited art for the following reasons.

Claim 99 (and thus claim 77) and claim 80 (and thus claims 86 and 87) are patentable over Menezes for the reasons set forth above. Claims 99, 100, and 80 are patentable over Pfleeger because Pfleeger fails to teach or suggest the above-noted limitations of claim 99, 100, or 80. Indeed, the Office Action does not take the position that Pfleeger teaches or suggests these limitations. Thus, claims 99, 100, and 80 (and dependent claims 77 and 86-87) are patentable over Menezes and Pfleeger, whether considered individually or in combination.

Claims 1-5, 8-26, 31-36, and 53-57 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Pfleeger. In response, Applicant contends that the uncanceled ones of these claims as amended, and new claims 88, 89, 90, 91, 92, 93 (and 94), and 98, which respectively replace claims 4, 11, 12, 16, 21, 31, 53, and 57, are patentable over the cited art for the following reasons.

Amended claim 2 recites a repeater including circuitry configured to be coupled to receive encrypted data from a transmitter, to decrypt the encrypted data to generate decrypted data, to generate translated data by processing the decrypted data, to generate re-encrypted data by encrypting the translated data, and to transmit the re-encrypted data over a TMDS-like link.

Claim 88 recites a repeater includes circuitry configured to be operable in an encryption mode to generate encrypted data by encrypting "first data" using a secret value and circuitry configured to generate the first data from "second encrypted data" including by decrypting the second encrypted data using a second secret value.

Pfleeger fails to teach or suggest a repeater of the type recited in amended claim 2

including a repeater having data translation and encryption capability as recited in amended claim 2 or a repeater of the type recited in claim 88 having decryption and re-encryption capability of the type recited in claim 88. Although Pfleeger's pages 386-387, 389, and 406 disclose or contemplate use of repeaters, there is no teaching or suggestion determinable from Pfleeger (at page 386, 387, 389, or 406, or elsewhere) that any repeater in any system or network disclosed in Pfleeger should have data translation and encryption capability as recited in claim 2 or decryption and re-encryption capability of the type recited in claim 88. Neither the cited text entitled "Link Encryption" at Pfleeger's page 406, nor other text in Pfleeger, teaches or suggests that an "intermediate host" (or any other device) should be operable or configured to generate decrypted data by decrypting encrypted data received from a transmitter, to generate translated data by processing the decrypted data, and to generate re-encrypted data by encrypting the translated data as recited in claim 2. Nor is there teaching or suggestion determinable from Pfleeger's page 406 (or elsewhere) that an "intermediate host" (or any other device) should be operable or configured to generate "first data" from second encrypted data (received from a content source) including by decrypting the second encrypted data using a second secret value and to generate encrypted data (for transmission to a third device) by encrypting the first data using another secret value (the "secret value" of claim 88) as recited in claim 88.

There is no teaching or suggestion determinable from Pfleeger's pages 131-132 (or elsewhere in Pfleeger) supporting the apparent assertion in paragraph 33 of the Office Action that a key exchange between two devices using a third device (a central key repository or other "external agent") as described at Pfleeger's pages 131-132 should employ a fourth device (e.g., a repeater) of any type, much less a fourth device that is a repeater operable or configured to generate "first data" from second encrypted data (received from a content source) including by decrypting the second encrypted data using a second secret value and to generate encrypted data (for transmission over a link) by encrypting the first data using another secret value (the "secret value" of claim 88) as recited in claim 88. Even if one assumes for the sake of argument that it would have been obvious to one of ordinary skill in the art (as of filing of the present application) to have included a repeater between any two of the three devices described at Pfleeger's pages 131-132 (Renee or Octavia, Pablo, and the central key repository), claim 88 is patentable over Pfleeger because there is no teaching or suggestion determinable from Pfleeger to employ for this purpose a repeater operable or configured to generate "first data" from second encrypted data (received from a content

source) including by decrypting the second encrypted data using a second secret value and to generate encrypted data (for transmission over a link) by encrypting the first data using another secret value (the "secret value" of claim 88) as recited in claim 88.

Claim 89 recites a transmitter including circuitry configured to be coupled to at least one TMDS-like link and operable in an encryption mode to generate encrypted data by encrypting first data using a sequence of secret values including a secret value and to transmit the encrypted data over the at least one TMDS-like link. Pfleeger fails to teach or suggest a transmitter of the type recited in claim 89.

Claim 90 recites a router including circuitry operable in a first mode and a second mode, wherein, in the first mode, the circuitry forwards to at least one additional serial link multiply encrypted data received from at least one serial link, and wherein, in the second mode, the circuitry generates encrypted data by performing a translation operation on multiply encrypted data received from the at least one serial link, wherein the translation operation includes decryption of the multiply encrypted data using a second secret value in accordance with a second content protection protocol, and forwards the encrypted data to the at least one additional serial link (for decryption by a receiver using a third secret value). Pfleeger fails to teach or suggest (either at page 262, cited in paragraph 34 of the Office Action, or elsewhere) a router of the type as recited in claim 90, or a communication system including such a router.

Claim 91 recites a translating router including circuitry of a specified type. Pfleeger fails to teach or suggest (either at page 262, cited in paragraph 34 of the Office Action, or elsewhere) a translating router of the type as recited in claim 91, or a communication system including such a translating router.

Claim 92 recites a repeater including circuitry configured to generate decrypted data including by decrypting encrypted data using a secret value, to generate re-encrypted data including by encrypting the decrypted data using a second secret value, and to transmit the re-encrypted data over second link. Pfleeger fails to teach or suggest a repeater of the type recited in claim 92, or a communication system including such a repeater.

Claim 93 recites a receiver including circuitry configured to be coupled to at least one

TMDS-like link, said receiver being configured to send to an external agent a ticket request including data indicative of at least one capability of the receiver. Claim 94 recites a transmitter including circuitry configured to be coupled to at least one TMDS-like link, said transmitter being configured to send to an external agent a ticket request including data indicative of at least one capability of a receiver coupled to the TMDS-like link. Pfleeger fails to teach or suggest (either at pages 131-132 or elsewhere) a transmitter or receiver configured to send to an external agent a ticket request including data indicative of at least one capability of a receiver as recited in claim 93 and 94, or a communication system including such a transmitter or receiver. Nor does Pfleeger teach or suggest such a transmitter or receiver configured to send a ticket request including data (indicative of at least one capability of a receiver) that indicates whether the receiver can assert digital data protected by a content protection protocol at an output of said receiver, as recited in claim 34 which depends from claim 93) or claim 96 (which depends from claim 94).

Claim 97 recites an external agent configured to be coupled to a transmitter and a receiver, wherein the external agent is configured to be operable in a mode in which it sends at least one signal to the receiver and at least one additional signal to the transmitter, wherein the at least one additional signal is indicative of at least one of a secret value, an encrypted version of the secret value, and data enabling the transmitter to obtain the secret value, and the at least one signal is indicative of first data and second data, wherein the first data comprise at least one of the secret value, an encrypted version of the secret value, and data enabling the receiver to obtain the secret value, and the second data includes a code value that identifies the secret key without revealing the secret key, and the secret key cannot be derived from the second data. Pfleeger fails to teach or suggest (either at pages 131-132 or elsewhere) an external agent configured to respond to a ticket request by sending at least one signal (of the type explicitly recited in claim 97) to a receiver and at least one additional signal (of the type explicitly recited in claim 97) to a transmitter as recited in claim 97, or a communication system including such an external agent.

Claim 98 recites an external agent configured to be coupled to a transmitter and a receiver, wherein the external agent is configured to be operable in a mode in which it sends at least one signal to the receiver and at least one additional signal to the transmitter, wherein the at least one additional signal is indicative of at least one of a secret value, an encrypted version of the secret value, and data enabling the transmitter to obtain the secret value, and is

also configured to be operable in a second mode in which it sends a control signal to the transmitter and a second control signal to the receiver, wherein the transmitter is configured to operate in a pass-through mode in response to the control signal and the receiver is configured to operate in a non-decrypting mode in response to the second control signal. Pfleeger fails to teach or suggest (either at pages 131-132 or elsewhere) an external agent that is configured to operate in a mode in which it sends signals (of the type explicitly recited in claim 98) to a transmitter and a receiver, and is operable in a second mode in which it sends a control signal (of the type explicitly recited in claim 98) to the transmitter and a second control signal (of the type explicitly recited in claim 98) to the receiver as recited in claim 98, or a communication system including such an external agent.

Claims 6-7 and 27-30 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Pfleeger in view of US Patent Application Publication No. 20030005285 ("Graunke"). In response, Applicant contends that these claims are patentable over the cited art for the following reasons.

Claims 6 and 7 are patentable over Pfleeger for the same reasons set forth above that claim 88 is patentable over Pfleeger. The Office Action identifies no teaching or suggestion in Graunke of a repeater having decryption and re-encryption capability of the type recited in claim 88. Thus, Applicant respectfully contends that claim 88 is (and thus claims 6 and 7are) patentable over Pfleeger and Graunke, considered individually or in combination.

Claims 27-30 are patentable over Pfleeger for the same reasons set forth above that claim 92 is patentable over Pfleeger. The Office Action identifies no teaching or suggestion in Graunke of a repeater of the type recited in claim 92. Thus, Applicant respectfully

contends that claim 92 is (and thus claims 27-30 are) patentable over Pfleeger and Graunke, considered individually or in combination.

Respectfully submitted,

GIRARD & EQUITZ LLP

Dated: 7/11/06 By: Alfred A. Equitz

Alfred A. Equitz
Reg. No. 30,922

Attorneys for Applicant

Attorney Docket No. SII-800 [SIMG0103]